

REMARKS/ARGUMENTS

The Office Action mailed December 1, 2003 has been reviewed and carefully considered. Claim 16 is amended. Claims 1-18 are pending in this application, with claims 1 and 6 being the only independent claims. Reconsideration of the above-identified application, in view of the following remarks, is respectfully requested.

In the Office Action mailed December 1, 2003, claims 1-4 and 6-9 stand rejected under 35 U.S.C. §103 as unpatentable over U.S. Patent No. 5,812,764 (Heinz) in view of U.S. Patent No. 6,223,292 (Dean).

Claims 5 and 10-11 stand rejected under 35 U.S.C. §103 as unpatentable over Heinz and Dean and further in view of U.S. Patent No. 6,006,333 (Nielson).

Claims 12-14 and 18 stand rejected under 35 U.S.C. §103 as unpatentable over Heinz and Dean and further in view of U.S. Patent No. 6,113,292 (Sormunen).

Claims 16-17 stand rejected under 35 U.S.C. §103 as unpatentable over Heinz and Dean and further in view of Sormunen and Nielsen.

Claim 16 is amended to correct a minor typographical error.

Claim 15 was found to contain allowable subject matter and was objected to as being dependent on a rejected base claim. While the finding of allowable subject matter is appreciated, the rejection of independent claims 1 and 6 is traversed in view of the following remarks.

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the present invention is appropriate. The present invention relates to a method and an arrangement for remotely accessing password protected services in a data communication system. The present invention is intended for use in systems in which a service

provider provides to a user of a service a number of expendable passwords, by means of which a user can access the service via telecommunication and/or data networks (see page 4, lines 12-15 of the specification). According to the invention, a user's telecommunication device includes a module which registers passwords transmitted from a service (page 8, lines 3-13). The module may save passwords for a variety of services (see, e.g., table 1 on page 10). When a user calls a service, the module refers to the list of services and passwords and determines whether the service being called by the user requires a password. If a password is required, the module automatically selects and adds a password to the setup signal or string for transmission to the server (see page 5, lines 1-2; and page 9, lines 14-18). The server receives the password in the signaling data provided through the telephone network (page 11, lines 1-2).

Independent claims 1 and 6 each specifically recite that the terminal device automatically selects a password and that the terminal device adds the password to the connection setup signal.

Heinz discloses a password management system for passwords used over a communication system. According to Heinz, a server generates a list of passwords which is saved in both the server and the client devices. A client initiates communication from the client device to the server, and the server responds by selecting a password (col. 5, lines 35-39). The server then informs the client of an identifier of the selected password (not the password), and the client then extracts the password from the list at the client device (col. 5, lines 55-59). Since Heinz requires the server to select the password in response to the client initiation of communication, Heinz fails to teach or suggest "selecting from the stored set of expendable passwords, automatically by the terminal device at user log-on to the service, one of the stored passwords for use in logging on to the service" and "transmitting the selected password to the server by adding the selected

password to a connection setup signal transmitted from the terminal device to the server via the network to remotely log-on to the service from the terminal device of the user", as expressly recited in applicants' independent claims 1 and 6. In contrast to the present invention, Heinz teaches that the client initially sends a connection setup signal without a password. Heinz furthermore teaches that the password is determined by the server and that the client device responds to that selection by the server.

Dean likewise fails to teach or suggest the selection of a password from a list of expendable passwords. Dean discloses an authorization system and method in which a computer sends a request for a service with a service differentiable password. According to Dean, the password is transmitted with a request for a service, wherein the password is indicative of a service level (col. 5, lines 31-37). The identified service level is the minimum service to be provided (col. 5, lines 37-39). Dean fails to teach or suggest that this password is an expendable password or that there is a list of passwords from which the client terminal automatically selects. In view of the foregoing, it is apparent that neither Heinz nor Dean teaches or suggests "selecting from the stored set of expendable passwords, automatically by the terminal device at user log-on to the service, one of the stored passwords for use in logging on to the service", as expressly recited in applicants' independent claims 1 and 6. It is therefore respectfully submitted that independent claims 1 and 6 are allowable over Heinz in view of Dean.

Dependent claims 2-5 and 7-18, each being dependent on one of independent claims 1 and 6, are deemed allowable for the same reasons expressed above with respect to independent claims 1 and 6.

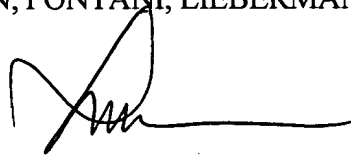
This application is now believed to be in condition for allowance, and early notice to that effect is solicited.



It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any such fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By 

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: March 24, 2004

RECEIVED

MAR 30 2004

Technology Center 2100